

VOTEFILER™ WHITEPAPER

Paper Ballots with Secure Electronic Tabulation



VOTEFILER OVERVIEW

This document describes a patented process for voting that combines the privacy of sealed paper ballots, the verifiability of a paper trail, and the high-speed efficiency of electronic voting. Voters who choose to take advantage of the system can create a paper ballot in advance of Election Day from any Internet-connected computer with a printer and then submit that ballot at a traditional voting station during regular voting hours.

Voters do not actually cast a ballot before Election Day; they create a secure and uniquely identified ballot that a bardode scanner can turn into votes at the polling station. It has two parts that are linked by the unique identifier:

- the paper ballot brought to the polling station on Election Day
- the electronic record of the selections, stored in a database

This system does not have to be an all-or-nothing solution imposed on voters. It can be phased in over multiple election cycles, if desired, and can coexist with other voting systems. As more voters embrace the ease of making voting choices when they have the time to do so thoughtfully, and at a convenient location such as their home or office, the VoteFiler solution will speed up the tabulation of votes while providing the security of a paper trail when required.

VoteFiler does not use proprietary voting machines that are used only a few days a year. Instead, an Election Official logs in to a secure website from an off-the-shelf personal computer that, in many cases, can be borrowed for the day from an office or classroom. If the voting jurisdiction decides to buy PCs or Macintosh computers specifically for Election Day, the cost is in the neighborhood of \$1000 per station, a big savings over other proposed systems.

For absentee and provisional ballots, where current procedures often compromise the secrecy of the votes, VoteFiler offers the advantage of a paper ballot that is separable from the personal information needed to authenticate the voter.

WHAT VOTEFILER IS

VoteFiler is a patented technology from Comfidex Corporation that combines the best features of traditional voting with the advantages of high-speed electronic vote tabulation. Here's a brief introduction to how it works.

Anyone can create a paper ballot during the days before an election by visiting a web site. Without asking for the person's identity, the web site uses geographical questions to determine the correct voting precinct for each user. A series of pages allows the voter to make a selection in each of the contests and ballot ques-

tions. The user prints a paper ballot on standard 8.5"x11" printer paper that includes both a human-readable list of all the selections and an encrypted barcode that uniquely identifies this ballot.

Before the document is printed, the selections are captured in a Ballot database that is connected to the web site's servers. The encrypted data in the barcode uniquely identifies each saved ballot and also contains integrity information that can protect against successful tampering with the database. Records in the Ballot database are not considered votes until the ballot is presented on Election Day. A user can later create a new ballot based on a change of preferences or even a need to replace a lost ballot. Ballots that are not presented to a Polling Station never become votes.

On Election Day, the user takes this ballot to the Polling Station. It is folded into a specially designed envelope that hides the clear text list of selections but reveals the barcode through a window in the envelope. The VoteFiler voter goes through the same authentication process as other voters and then, instead of being directed to a line for a voting booth, hands the sealed envelope to an Election Official who quickly scans the barcode. VoteFiler provides the equivalent of the express line at the supermarket.

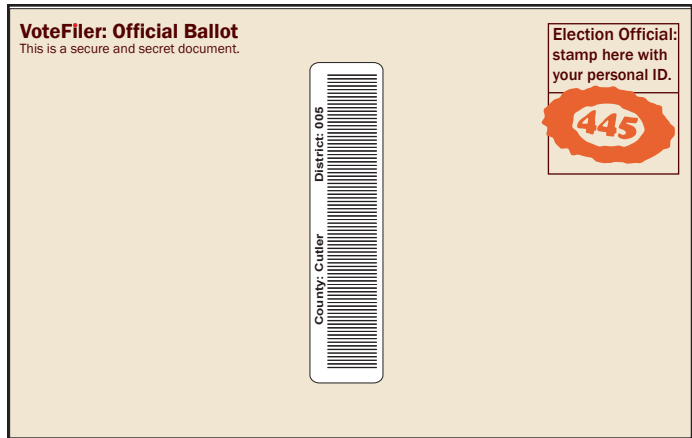


Figure 1: The ballot in its envelope.

If this is a valid ballot—that is, the scanned barcode identifies an authentic, unused record in the Ballot database—then all selections become votes in a separate Votes database and the voter is done; there's no second line to wait in. The Election Official stamps the outside of the VoteFiler envelope to identify which official accepted the ballot and he or she places it in a ballot box.

After the polls close, the votes are tallied from the Votes database. These totals are added to the counts from other voting methods to arrive at the final vote counts.

If the ballots need to be audited or recounted for any reason, a paper trail exists in all the locked ballot boxes. If the ballot envelopes need to be opened, the choices are in clear, unambiguous, computer-printed text in a consistent font and layout.

VOTEFILER IS DIFFERENT FROM OTHER ELECTRONIC VOTING

VoteFiler is not a voting machine. It is a technology that enables voters to:

- Make voting decisions on a computer at home, in the office, or at any computer with an Internet connection and a printer
- Hand the appropriate Election Official at a Polling Station a secret, ready-to-be-scanned, recountable paper ballot on Election Day, without waiting for a voting booth

At both stages—creating the ballot and reading the ballot—any off-the-shelf hardware can be used. Likewise, no proprietary software is required at either of these locations, only a standard web browser. All of the functionality of VoteFiler is implemented at the web servers and database servers that accept and manage the individual ballots.

text continued on page 4

SIDEBAR: THE FLOW OF INFORMATION IN VOTEFILER

In VoteFiler, data moves in a way that makes it easy for voters to create ballots while preserving the secrecy and integrity of individual votes. Where data passes through the public Internet, the Secure Sockets Layer (SSL), data encryption, and redundancy safeguards collaborate to make the creation of ballots secure. Plus, only records that meet the highest standards of authentication can be used on Election Day to create actual votes.

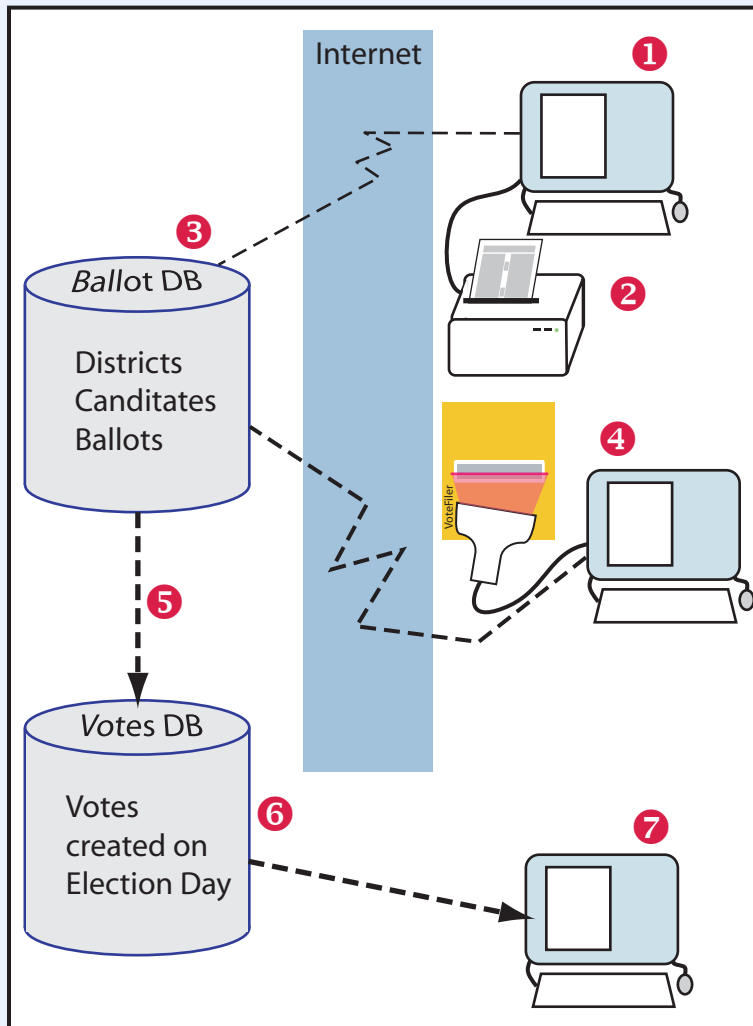


Figure 2: Data flow

the Internet to the Ballot database. If the unique identifier is validated as an unused ballot, the votes are transferred **5** to the Votes database with no record of who cast the vote. The sealed envelope is then placed in a locked ballot box.

At the end of Election Day, the Votes database tabulates totals for all races and ballot questions. **6** At Election Headquarters, **7** the results are added to the results from other voting methods to arrive at the final tallies. Note that the Votes database is not connected to the Internet; the connection between the two databases is only an internal network that has the Votes database behind a firewall.

(SSL), data encryption, and redundancy safeguards collaborate to make the creation of ballots secure. Plus, only records that meet the highest standards of authentication can be used on Election Day to create actual votes.

During a predefined period before Election Day, voters visit a web site **1** that has access to the Ballot database. The browser automatically shifts to secure mode using SSL to transfer all data securely to the web server and its database. On the home computer, all selections are kept only in memory, not stored on the local hard drive, which preserves the secrecy of the ballot.

Once the user has finished creating a ballot, two things happen: First, a printable version appears on the screen and **2** the user prints it locally. Second, the ballot's data is sent to the Ballot Database where it is stored electronically **3** as a database record in XML format.

On Election Day, after the voter has been authenticated at the polling station, he or she hands the ballot, folded into a special envelope, to the Election Official. The official ballot's barcode is scanned **4** and its data is sent across

The cost to local Election Boards is small or nil, because off-the-shelf computers with Internet connections are all that is needed. In contrast, the cost of proprietary hardware and software used in other systems can be substantial. Where a state needs to buy equipment for dozens or even hundreds of precincts, the VoteFiler approach can save the state millions of dollars. Even factoring in the costs of setting up and running the servers and data center, VoteFiler is significantly cheaper.

There are two other ways that VoteFiler differs significantly from proprietary voting machines:

- Voters are not confronted with a new experience on Election Day that is potentially intimidating and confusing. Choices are made at the voters' leisure before Election Day, when they can take the time to figure out the process, figure out who and what they want to vote for, and seek assistance if they choose to. On Election Day, all they have to do is sign in at the polling station and hand the preprinted ballot to the Election Official.
- Voters have a choice whether to use VoteFiler. For any reason, and with no need to provide an explanation, they can opt to use a voting booth.

HOW DIFFERENT USERS PERCEIVE VOTEFILER

The Experience of Voters

During some fixed period of days before Election Day, any voter can go to a web site that has been set up to create and record paper ballots. These are not votes being generated, only filled-in ballots. The user enters his or her local election district, if known, or else answers questions about the general location so that the district can be determined. At no time does the visitor to the web site state his or her identity or provide an exact address from which the identity can be inferred.

Based on the district chosen, the user is presented with a series of screens, one for each contest being voted on. On each page, voters have a choice between selecting a candidate, writing in a name, or abstaining. At the end, the ballot's creator sees a summary of his or her selections in all races, ballot initiatives, and other contests being put to a vote. The user has the option of returning to any pages that need to be changed. Once all votes are as the user wants them, the ballot is submitted, and two things happen:

- The selections are stored in a database (more about this below).
- A printable version of the ballot appears on the computer screen. It has all selections printed in clear and unambiguous human-readable text. In addition, the page includes a unique and encrypted identifier displayed as a barcode.

The user prints a copy of the ballot to submit on Election Day, and can print another copy as a personal record, if desired. (Note that duplicates cannot be used to vote. Once a ballot's unique identifier has been submitted, it cannot be used again.)

If, at a later time before Election Day, the user wants to change a vote, it is possible to return to the web site and create a new ballot. Unused ballots are not votes.

On Election Day, the voter takes the paper ballot to the Polling Station. If he or she has already picked up a VoteFiler envelope from one of the public locations where the election board has made them available, the ballot can be already sealed inside. Otherwise, envelopes are available at the polling station. The ballot is folded in such a way that the human-readable text is hidden inside the sealed envelope; only the barcode, the election district name, and the date are visible. There is no indication of who the voter is either inside or outside the envelope.

The voter signs in as usual. All the existing safeguards to ensure that only registered voters vote and that no one votes more than once remain. Once authenticated, the voter hands the sealed envelope to the Election

Official who scans the barcode. The barcode reader is attached to a computer, which transmits the unique identifier to a database in which the electronic part of the ballot is stored. If the indication comes back that the ballot is valid—and unused—then the selections on the ballot are turned into votes, and the voter is finished, with no need to wait for a voting machine to become available.

The Election Official places the sealed ballot in a locked ballot box in case it's needed again in a recount.

The Experience of Poll Workers

While each voting station requires the same number of workers validating voters as before, it may require fewer voting machines of whatever type: punch card, lever, electronic voting booth, and so on. More of the Election Day volunteers can be assigned to the lines of voters waiting to sign in, possibly reducing overall wait times.

Each Election Official logs in with a personal password to the database that serves this polling station. All votes cast with VoteFiler ballots during his or her watch are stamped on the outside of the envelope to identify the Election Official who accepted it. In case of an audit or recount, the total of paper ballots with his or her stamp can be compared to the number of ballots submitted electronically under that login name; this accountability for Election Officials is a possible deterrent against fraud at the polling station.

After a voter has been validated, he or she is given a choice of using a VoteFiler paper ballot or whatever other method is in use in that district. No one is forced to use the new voting method. Those who select the traditional method are directed to the line of those waiting for a voting booth. The others hand their sealed envelope to an Election Official who uses the computer-attached scanner to read the encrypted barcode. A nearly instantaneous response indicates whether the ballot is valid. If it is, the Election Official stamps the exterior of the envelope with a personal stamp. The sealed envelope is then placed in a locked ballot box, and that vote has been cast. These envelopes containing the paper ballots should be retained under lock and key in case a recount is later required.

In the unlikely case that the ballot is not accepted—including an inability to contact the database—the user is informed that the ballot cannot be read, and the user is invited to vote by the more traditional method. (The voter can open the envelope, if desired, to use the text on the ballot as a reminder of his or her choices.)

The reasons that a ballot would not be accepted include:

1. The polls are not currently open.
2. A ballot with this ID has already been submitted. This event could occur innocently because a voter mistakenly thinks it is possible to photocopy another's ballot.
3. The unique identifier on the ballot is not valid.

The Experience of Recounters

There are various levels of audits and recounts, depending on what is being questioned:

1. Election officials can routinely count the unopened envelopes to make sure the number of ballots recorded in the database for the precinct matches the number of actual ballots submitted. Furthermore, the count during each Election Official's watch can be verified so that, if there is a discrepancy, the problem can be narrowed to specific personnel.
2. Ballots can be rescanned after the close of polls to verify that there's a one-to-one match between votes cast and votes tabulated. This rescan can be done either across an entire jurisdiction, or to some randomly selected precincts.

3. If the ballots are opened, the option exists to use OCR technology (Optical Character Recognition). This approach increases the speed and accuracy over human readers. Even though unconstrained OCR is not currently 100% accurate, if the OCR scan only has to distinguish between, for example, “James Harris” and “Barbara Smith,” automated context analysis can correct any misreads of individual characters, creating 100% confidence in the results.
4. The most extensive recount is to open all ballot envelopes, read the clear-text votes, and tabulate the results by hand. This level of recount should only be necessary if someone questions the electronically tabulated totals. This recount can be performed for a single contest, or for all contests on the ballot.

Note that there is no indication anywhere inside or outside the envelope of who submitted a ballot; the secrecy of the voting process is preserved. Even absentee ballots, that under other systems often have name and address on the same large sheet as the preferences, are totally anonymous during a VoteFiler recount.

The Experience of Absentee Voters

VoteFiler simplifies voting for those who cannot make it to their assigned voting location on Election Day and, in addition, provides them a more private ballot than most traditional absentee ballots.

Absentee voters who select to use the VoteFiler web site generate a paper ballot the same as everyone else. And they request an absentee ballot the same as anyone else in that voting district. Where the absentee ballot requests identifying information, such as name and address, and a signature, the data is filled in on the form. But, instead of marking selections directly on the form, the voter includes the printed ballot, in its specially designed envelope, with the absentee ballot. The whole package is now mailed—or otherwise delivered—to wherever all absentee ballots go.

If absentee ballots are opened and authenticated before Election Day, then VoteFiler can correct the current problem that most of these ballots are not counted unless the difference between the top candidate totals is small enough that the absentee ballots might affect the outcome. These ballots can be quickly scanned on Election Day and become part of the same-day results.

The Experience of Provisional Voters

When a person’s qualification to vote is questioned at the polling station, and that question cannot be resolved quickly, the person is given a provisional ballot, often a packet in which identifying information is attached to the paper form on which the users indicates his or her choices. This approach can compromise the secrecy of the potential voter’s ballot.

With VoteFiler, the sealed envelope is attached to the identifying information. If the person is accepted as a registered voter, then the barcode is scanned and the ballot’s contents remain private.

The Experience of Counters for Absentee and Provisional Voting

Those who open incoming absentee and provisional ballots divide them into two groups: those using VoteFiler ballots and those using only the hand-marked forms. The latter group can be processed as in the past.

Those containing a VoteFiler envelope are first checked against voting rolls using the personal data on the standard form. If accepted, the barcode is scanned to cast the votes. The Election Official presiding at the qualification of the voters stamps the outside of the VoteFiler envelope, and places it in the locked ballot

text continued on page 8

State: Kansas

County: Cutler

District: 005

November 7, 2006

Instructions: For your vote to be counted, you must either (a) bring this ballot to the District 5 Polling Station at the address below on Election Day or (b) follow the instructions for mailing this ballot as an absentee ballot. In either case, you will need to fold this ballot along the dotted line in the middle of the page so that the printing appears on the outside. When placed in the special VoteFiler envelope, the one of the barcodes must appear in the window.

Poll Address:
345 Hamden St. (at Gracey Blvd.)

President & Vice President
Ian Conroy & Joan Smith (Democratic Party)

U.S. Senator
Brian Jones (Republican Party)

U.S. Representative
Christine Wu (Democratic Party)

Kansas State Senator
Chris Nigel (Conservative Party)

Kansas State Representative
Leslie Klein (Republican Party)

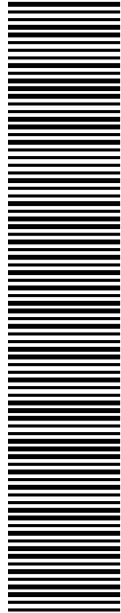
Mayor of Farmview
Bruce Durham (Republican Party)

District Judges
Ben Dorgan (Democratic Party)
Ken Smithers (Democratic Party)
Heather Tyne (Libertarian Party)

Education Director
Wendy Cole (Republican Party)

Parks Commissioner
Michael Greene (Democratic Party)

School Board
Aaron Adams (Democratic Party)
Wanda Asthamaya (Green Party)
Lance Gold (Liberal Party)
Bernice Obonowski (Democratic Party)
Elise Thayers (Republican Party)



County: Cutler District: 005



County: Cutler District: 005

Question:
State Educational Bond: whether to permit the sale of bonds for school repairs
Yes

Question:
Mayor's Tenure: whether to restrict any mayor to no more than two (2) terms in office
No

Figure 3: Sample Ballot

box. The identifying data has been separated from the ballot, better preserving the secrecy of the votes should the ballot become part of a recount. This process is much faster, and less error-prone than reading hand-marked forms. Each electoral jurisdiction can decide whether to include these immediately available numbers in the Election Day totals, or wait to include them with other late results.

The Experience of Database Administrators

Ballots and votes are stored in separate databases. A ballot record is created each time a user visits the site and submits a set of selections. It does not matter how many times a user changes his or her mind, only the one ballot submitted on Election Day becomes an entry in the Voting database. The counts in this database have no intrinsic meaning, and should never be revealed.

When the polls close in each voting district, votes can be quickly tabulated from a single database. At first, not all votes will be cast using VoteFiler, so total result will have to wait to include other counts. But, because fewer votes are cast by the more traditional means, that counting might proceed more quickly, as well.

Each state can decide whether to use a state-wide pair of databases, or to subdivide the state, or even to share a database with other states. The scope of any VoteFiler election system makes little difference to the design.

VoteFiler can include programs that run against the Ballots database searching for tampering. Records are designed with multiple integrity guarantees. Details of the safeguards are not discussed here. No man-made system can be consider 100% tamper-proof; multiple integrity routines make VoteFiler highly tamper-evident, before, during, and after Election Day.

The Experience of Would-Be Hackers

It is virtually impossible to tamper successfully with the database of ballots. That's because the encrypted barcodes contain not only a unique identifier, but also enough specifics about the aggregate of selections that any change to either the barcode or the selections will create a mismatch that can be detected at the time the barcode is decrypted.

Anyone who tried to change a ballot item to indicate a selection of votes different from what the user selected online, but leave the information in the barcode intact, would make the ballot invalid. When the ballot is presented at the polling station, the software running at the database decodes the barcode and compares it to the encrypted information about selections contained in it. If the two do not match, the ballot is not accepted. (Actually, such comparisons can be run routinely before Election Day to search for such malfeasance, and steps taken—such as looking at backup copies of the database—to try to rectify the problem in advance.)

Another attempt at hacking might be to try to create a new record in the databases, and create matching ballots—perhaps with false selections in the human-readable text, in the hope of giving the ballots to unsuspecting voters. Because of the wide spacing between used numerical identifiers and the encryption of the data in the barcode, the chance of generating a valid barcode is one-in-many-millions, or worse.

A third attempt might be to try to create votes in the Votes database that are not in the Ballot database. Constant reconciliation of the two databases—both on and after Election Day—will find any such attempt very quickly. Plus, the Votes database is not accessible via the Internet, meaning that a hacker would have

to have direct access to this database during the limited number of hours that votes are being written to this database.

The ultimate security feature—and a prospect that would dissuade most from even attempting to hack into the database—is the fact that the paper ballots are the official ballots. If the database records appear to be tampered with in any way, the affected districts will resort to the paper ballots. Tampering can be discovered from internal integrity checks, or from random audits that compare the database records with the paper records in a few sample precincts.

A SAMPLE BALLOT

Figure 3, on page 7, displays a typical ballot. Each voter’s choices are spelled out in clear and unambiguous text, and the duplicate barcodes down the center encode an identifier unique to this ballot. Nothing on the ballot identifies the voter in any way.

Once the voter has printed the ballot, it needs to be folded in half and inserted in a specially provided window envelope. This will be available at the polling station, and can also be provided before Election Day in public locations, such as post offices, banks, and government buildings. When folded, the ballot looks like the diagram in Figure 4.

It is then inserted in a specially designed window envelope that reveals the barcode but not the clear-text choices. The voter seals the envelope. Only the district name, the date, and the barcode are visible. Figure 1 shows the sealed envelope, with the Election Official’s stamp in the upper right corner. Election Boards can also make these special envelopes available in advance of Election Day in public locations such as post offices and town halls, if desired. Being able to seal the ballot envelope at home can reduce any voter’s concern that others will see the printed selections while at the Polling Station.

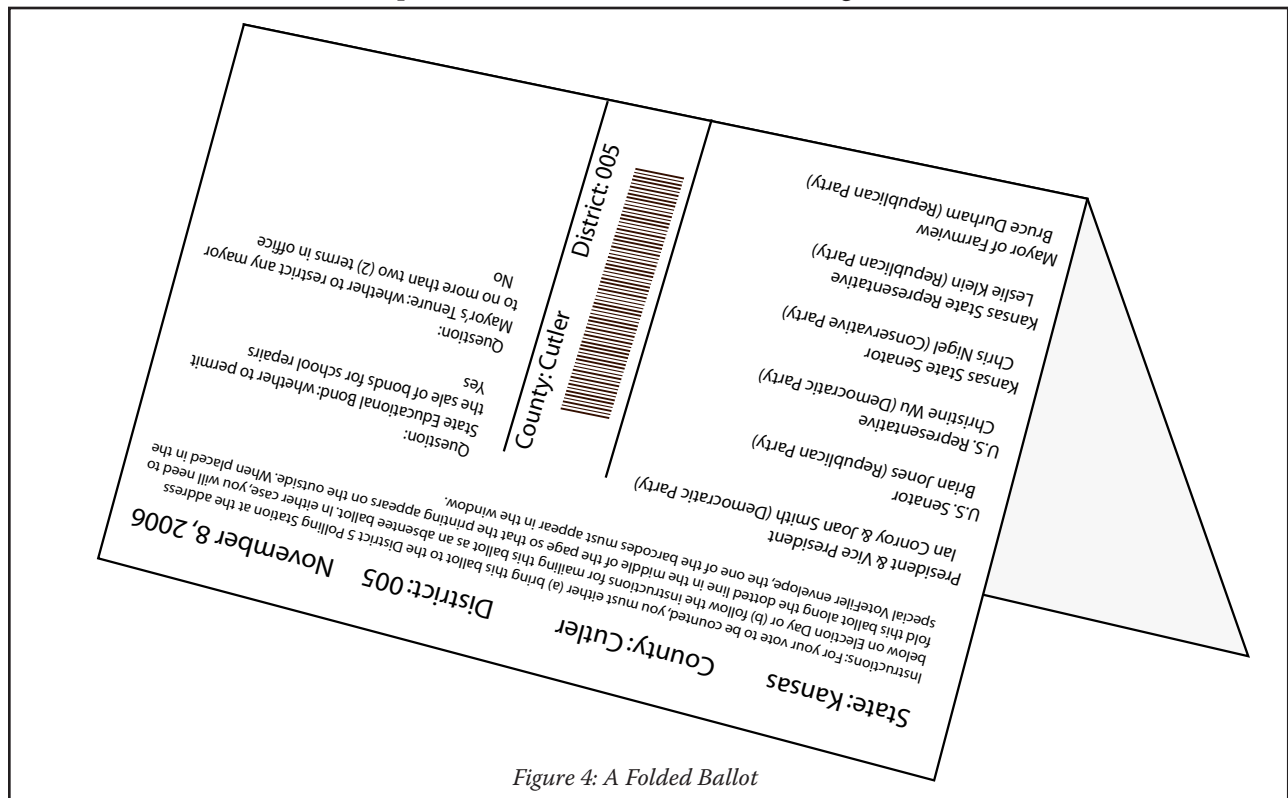


Figure 4: A Folded Ballot

ADMINISTERING THE DATABASE OF CANDIDATES

Before the web site is opened to allow the creation of VoteFiler ballots, information about the voting districts, the various contests, and the names of the candidates running in each race must be entered into the Ballot database. Two goals drive the design of this functionality:

- The process should avoid double-keying of information into separate databases—the state’s database (if any) plus the VoteFiler database.
- Different states and/or local election boards may have very different systems for storing this information locally.

Therefore, VoteFiler is designed to import data directly from files that can be easily exported from existing state systems.

A direct user interface to this information also exists so that those administering an election can make last-minutes changes. This could be required to accommodate a judicial ruling that adds or removes a candidate’s name based on an appeal.

ADMINISTERING THE RESULTS

Once the polls close in each voting district, the results need to be tallied from the Votes database. The VoteFiler system uses a program that runs attached to the database server to perform and monitor these tabulations, and to display the results. The vote tallies for each candidate can be viewed at various levels, including state-wide, county-wide, and per voting district. These results can then be printed to paper in a variety of formats.

Results can be retabulated at any time based on recounts, appeals, or other factors that may change the totals. These retabulations can be performed selectively on any specified list of voting districts.

The design of VoteFiler does not include the transmission of results to other computers. For security reasons, the servers that support the Votes database should have as few external connections as possible. The only connection is the secure network between the Ballot database and the Votes database. Local election headquarters can receive their results by fax, telephone, or other means, but there is no direct electronic link between the Votes database and any non-local computer.

The totals from the VoteFiler system are added to the totals from parallel voting systems for a final count.

HANDLING ERRORS

In any system, unexpected events ranging from hardware malfunction to an “Act of God” can disrupt even the best designed flow of data. A successfully designed system has safeguards in place to handle and correct any such disruptions efficiently.

Errors During Ballot Creation

If a problem occurs at the web site before the ballot is finalized, no ballot is created and no errors are introduced into the system. There is no such thing as an incomplete ballot. Once a ballot is transmitted to the server, it is checked for consistency. In the unlikely event that an internal problem is found in the ballot, the user is notified that the ballot cannot be created. Any failed attempt to create a ballot is recorded to a log file for review by system administrators. Bottom line: no incomplete or inconsistent ballots are generated.

Errors During Election Day Voting

When a ballot is scanned, the server tests the validity of both the barcode and the Ballot database record referenced in the barcode. If there is any problem, the ballot is rejected and the voter may use another means for voting. An error report is logged in the database.

The ballot is accepted before the ballot is sent to the Votes database. That's because there may be delays during high-volume periods and the ballots will be queued up for delivery. If the ballot cannot be delivered to the Votes database—because of a communications failure or any other problem—then the ballot is marked as undelivered and an error report is added to the log table. If the delivery of ballots times out, then an administrator can rectify the problem and resend any undelivered ballots. Bottom line: no votes are lost, though in a worst case scenario it may take an administrator's intervention to complete the transactions.

The Ultimate Backup: The Paper Ballots

No matter what unlikely disruption one can imagine at the servers, the paper ballots at the polling stations provide a fail-safe record of all votes cast using the VoteFiler system.

SUMMARY

VoteFiler is a system designed to make voting easier, more efficient, and more secure than other systems in use or being proposed. It addresses the many calls for an unambiguous paper trail while providing the speed and accuracy of electronic computing. It retains the face-to-face authentication of voters on Election Day while providing for the modern ease of making choices online at one's leisure. And, unlike many new voting systems, VoteFiler uses low-cost, commodity item components to provide an affordable solution.

VoteFiler is a twenty-first century voting method that retains the time-tested security of paper ballots.